

UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF TENNESSEE  
AT KNOXVILLE

IN THE MATTER OF THE SEARCH OF  
INFORMATION ASSOCIATED WITH  
badtrucking@icloud.com THAT IS STORED  
AT PREMISES CONTROLLED BY APPLE,  
INC.

Case No. 3:20-mj-2125

Filed Under Seal

**AFFIDAVIT IN SUPPORT OF  
AN APPLICATION FOR A SEARCH WARRANT**

I, J. Jason Pack, being first duly sworn, hereby depose and state as follows:

**INTRODUCTION AND AGENT BACKGROUND**

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple, Inc. (hereafter “Apple”) to disclose to the government records and other information, including the contents of communications, associated with the above-listed Apple ID that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent assigned to the Federal Bureau of Investigation’s (FBI) Knoxville Field Office. My current assignment includes investigating violent crime and crimes against children. I have served as an FBI agent for more than 16 years. During that time, I have received training in violations of federal law. I have served as the case agent in the execution of multiple search and arrest warrants during my service and have also worked alongside other agents and local officers in their investigations. I am one of only approximately 75 agents in the FBI selected to serve on the FBI’s highly specialized Child Abduction Rapid Deployment Team.

This team's specialty is locating missing children and investigating child abductions. I have also received extensive training in the use of online communications by those individuals with a sexual interest in children. I graduated from Carson-Newman College in 1992 with a journalism degree and have worked for fire and emergency medical departments, broadcast media outlets and the Federal Emergency Management Agency (FEMA) prior to joining the FBI. As a federal agent, I am authorized to investigate violations of laws of the United States and, as a federal law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that Everett Eugene Miller ("Miller") has transported a minor in interstate commerce with intent for the minor to engage in sexual activity for which a person can be charged with a criminal offense in violation 18 U.S.C. § 2423(a) and there is probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, or fruits of these crimes, as further described in Attachment B.

#### **JURISDICTION**

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), and (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

## PROBABLE CAUSE

### Tip to the Morgan County Sheriff's Office

6. On 1/27/2020 at approximately 12:30 p.m., Crystal Angel, sex offender coordinator at the Morgan County Sheriff's Office (MCSO), received an anonymous telephone call. The caller reported that Miller, a registered sex offender, had been transporting a 15-year-old female across state lines while Miller was working as a long-haul truck driver. The caller then identified other potential witnesses to the crime and provided contact information for the mother of the victim. Crystal Angel informed MCSO detectives concerning this tip.

### Victim's Mother's Statement to Police

7. On 1/30/2020, [REDACTED] walked into Morgan County Sheriff's Office and asked to file a police report concerning the sexual assault of [REDACTED] (the victim).

8. According to [REDACTED] statement Miller, [REDACTED], who goes by the nickname "EJ," had been having an "unhealthy" relationship with the victim. Miller is a semi-truck driver and he had taken the victim on several interstate trips in his the truck.

9. One of the trips [REDACTED] recalled was between on or about 6/30/2019 and 7/05/2019. Miller transported the victim alone in his truck from Sunbright, Tennessee (located in the Eastern District of Tennessee) through several states, eventually arriving in Salt Lake City, Utah.

10. Another trip described by [REDACTED] in which Miller travelled with the victim was on or about 12/22/2020. Miller transported the victim in his truck from Sunbright, Tennessee through several states, eventually arriving in Florida. On this trip, [REDACTED] said the victim was supposed to ride with Miller's wife, who is also a long-haul truck driver, while Miller followed behind in another semi-truck. However, the victim rode with Miller instead of Miller's wife.

When they arrived in Florida, their load was not ready, and Miller, his wife, and the victim had to return to Tennessee in the same truck.

11. The third trip taken by Miller alone with the victim occurred on 12/29/2019. This was supposed to be another "down and back" trip to Florida. However, Miller and the victim informed [REDACTED] the "back haul" from Florida was cancelled and the trip was changed to New Mexico.

12. On 1/26/2020 [REDACTED]  
[REDACTED] observed Miller standing behind the victim and assisting the victim with preparing food while laying his hand on top of the victim's hand and helped the victim stir macaroni and cheese.

13. The next day Miller's wife informed [REDACTED] that someone had made an anonymous tip to the MCSO concerning Miller transporting the victim across state lines. In response to this information, [REDACTED] confronted the victim [REDACTED] about their interactions with Miller and encouraged them to be honest with law enforcement or social workers should they come asking questions about interactions with Miller.

14. [REDACTED] asked the victim about [REDACTED] communication with Miller. [REDACTED] had previously observed 130 or more messages per day between the victim and Miller. [REDACTED] checked the victim's text messages and there were no text messages between the victim and Miller. [REDACTED] asked the victim how the victim and Miller were communicating now. The victim told [REDACTED] that Miller had purchased an iPhone for the victim to use to continue their messaging. [REDACTED] made the victim retrieve the iPhone provided by Miller and open it for [REDACTED] review.

15. During [REDACTED] brief review of the iPhone that Miller had provided to the victim, [REDACTED] saw a photo of the victim in [REDACTED] and what Stevens believed to be the top of Miller's blue jeans. [REDACTED] immediately closed the phone and took the victim to MCSO to file a police report.

16. [REDACTED] voluntarily surrendered both the victim's phone (a Samsung Android smart phone) and the Apple iPhone 7 that Miller had provided to the victim to MCSO. [REDACTED] provided MCSO with written consent to search the phones and with the passcodes to both phones. The victim's phones were further described by the following identifiers:

Secret Phone: (865) 250-[REDACTED]; Apple iPhone 7	IMEI: 35491609292716- Verizon Wireless
Samsung Android: (423) 215-[REDACTED]	IMEI: 352716086922130- Verizon Wireless

17. After leaving the MCSO [REDACTED] took the victim to the Morgan County Medical Center for evaluation of sexually transmitted diseases.

#### Forensic Interview of Victim

On 1/30/2020, the victim was interviewed at the Child Advocacy Center (CAC) in Lenoir City, Tennessee. The CAC interviewer presented the victim with a photograph of text messages observed by the MCSO review of the Apple iPhone 7 surrendered by [REDACTED]. The victim identified those messages as texts between [REDACTED] and Miller. The victim indicated that [REDACTED] and Miller had been text messaging for several months. Family members did not approve of their contact. Miller is the [REDACTED]  
[REDACTED]. Miller and his wife had been living [REDACTED]  
[REDACTED] in Sunbright, Tennessee, since 2017 or 2018.

18. The victim noted [REDACTED] relationship with Miller changed around Christmas 2019 when Miller took the victim in Miller's long-haul truck throughout the United States. Miller told the victim he wanted [REDACTED] with him "24-7". [REDACTED] disclosed to the interviewer that the victim [REDACTED] [REDACTED] to Miller while they were traveling outside the State of Tennessee.

19. The victim disclosed that the victim had sexual intercourse with Miller twice, both while on trips in the truck with Miller. The first time Miller had sex with the victim was during a trip to Salt Lake City, Utah. The second time the Miller had sex with the victim in New Mexico. During the trip to Utah, Miller pulled into a truck stop prior to arriving in Salt Lake City. The victim thought they were going to bed, but Miller decided to have sex and told the victim to be quiet. Miller took all his clothes off and unzipped the victim's pants. Miller laid on top of the victim and had sex with the victim. Miller also had the victim perform oral sex on Miller on more than one occasion, possibly twice. Miller frequently performed oral sex on the victim.

20. According to the victim, Miller's truck has a "bunker area" with bunk style beds and two front seats. The victim further disclosed Miller performed oral sex on the victim "as much as he wanted to" while they were traveling from state to state. Miller told the victim not to tell anyone, but never hit the victim.

21. The victim told [REDACTED] about the situation prior to the forensic interview. The victim stated that the victim's mother was suspicious because the victim and Miller were spending a lot of time together. The victim knew that Miller had been caught with minors previously, but did not know any specifics. Miller has since threatened to kill everyone who lives in the victim's home because someone reported him concerning sexual contact with the victim.

**Miller's Sexual Criminal History Regarding Sexual Assaults**

22. On 1/31/2020, William Angel, Assistant Chief Deputy at the MCSO, contacted me and requested investigative assistance from the FBI to determine if a Miller had committed a federal offense.

23. According to the Tennessee Bureau of Investigation's sex offender website, Miller is a violent sex offender. Miller's criminal history record from the National Crime Information Center, a commonly used law enforcement database that warehouses this information, indicates that Miller has arrests for sexual assault, rape, sexual battery by an authority figure and multiple probation and sex offender registry violations dating back to 1990.

24. According to criminal convictions that I have obtained, on 2/03/2003, Miller was convicted of the Sexual Battery by an Authority Figure and was sentenced to three years confinement. On 2/26/2009, Miller was convicted of violating Tennessee's Sex Offender Registry law and was sentenced to serve a year on probation.

#### **Arrest Warrant Obtained for Miller**

25. As a result of [REDACTED] complaint and a review of the evidence, MCSO obtained an arrest warrant for Miller for violating Tennessee Code Annotated, Section 40-39-211(c), Violation of the Sex Offender Registration Law. According to the Affidavit of Complaint supporting the warrant, Miller knowingly [REDACTED] the victim [REDACTED] since approximately November 2017 and took the minor victim alone with him on trips to Utah, Florida and New Mexico and for providing the victim a wireless phone without consent or knowledge of the minor's mother. The Affidavit of Complaint also referenced text messages between Miller and the victim which indicated an ongoing romantic relationship between Miller and the victim.

26. On 2/2/2020, Morgan County deputies arrested Miller at his home in Sunbright, Tennessee. Miller was released the same day after posting a \$30,000 bond. After Miller's arrest, investigators obtained a state search warrant for Miller's iPhone and requested investigative and technical assistance from the FBI.

27. Pursuant to MCSO's request and consistent with the terms of the state search warrant, the FBI took custody of Miller's iPhone to conduct a forensic examination. According to the forensic report, Miller's device was identified as a gray model A163 Apple iPhone 8, IMEI 35321810304687. The phone number associated with the device is 865-209-██████. The Apple ID associated with the device is: badtrucking@icloud.com. The application "Life360" was located also on the device, utilizing the email address: badtrucking@icloud.com to register.

28. Images that appear to be "selfies" of the victim were forensically recovered from Miller's iPhone. Some of those images were discovered to have been synced with the iCloud account badtrucking@icloud.com. An additional image of the victim's report card was also located on Miller's phone. That photo was identified through embedded metadata as being taken with an iPhone 7 on 01/9/2020.

29. A review of text messages on the Miller's iPhone contained the phone numbers 423-215-██████ and 865-250-██████. Both numbers are associated with the victim. The contact for the number 865-250-██████ was saved in Miller's phone with the victim's first name and a fictitious last name. There were no photographs containing child pornography located on Miller's iPhone.



**Subpoenas for Records Related to Miller**

30. In February 2020, I served Administrative subpoenas for business records related to Everett Miller to West Knoxville Transport, Life360, Apple, Inc. and Verizon Wireless for the following phone numbers:

423-215-██████
865-209-██████
865-250-██████
865-296-██████

31. Verizon responded to the subpoena with the following information:

423-215-0395	Registered Owner: ██████████ ██████████ Sunbright, TN
865-209-2987	Registered Owner: Everett Miller, 176 Red Hill Road, Sunbright, TN
865-250-2671	Registered Owner: Everett Miller, 176 Red Hill Road, Sunbright, TN
865-296-3588	Registered Owner: Bridgett Miller, 176 Red Hill Road, Sunbright, TN

32. On 2/28/2020, Life360 responded with the following information:

User: badtrucking@icloud.com	Subscriber: Everett Miller
------------------------------	----------------------------

33. On 2/20/2020, Avni Hashani, owner of West Knoxville Transport, provided the following information regarding Miller's employment. Hashani confirmed Miller drives truck number 286, a blue 2016 Freightliner truck. Hashani provided Miller's paystubs, fuel receipts, and driver logs for approximately the past six months, including two fuel receipts dated

08/17/2019 and 09/23/2019 from Sapp Brothers, located at 1953 California Avenue, Salt Lake City, Utah. There was also a fuel receipt dated 12/22/2019 from the Travel Centers of America in Knoxville. A review of Miller's driver's logbook provided by the company showed him listed in vacation status from 12/22/2019 through the end of the year.

34. On 5/10/2020, Hashani provided information pertaining to mileage sheets for Miller's truck that are consistent with the trips described by [REDACTED]. Among the trips reflected on the mileage sheets were the following:

- a. On 12/23/2019, Miller travelled from Knoxville to Lake City, Florida;
- b. On 1/6/2020, Miller departed Knoxville for Salt Lake City, Utah and delivered a load of freight back to Lake City, Florida; and
- c. On 1/8/2020, Miller picked up a load of freight in Loudon, Tennessee and delivered it to Albuquerque, New Mexico. On 1/9/2020, Miller departed New Mexico for Muleshoe, Texas and back to Conover, North Carolina.

According to Hashani, Miller drove Unit 286, the blue Freightliner truck for all of these trips.

35. As previously stated above, [REDACTED] recalled several trips, including a trip to New Mexico at approximately the same time the mileage sheet reflects Miller is driving the company truck in the same state. Additionally, the minor victim disclosed to a child forensic interviewer that Miller sexually assaulted [REDACTED] in both Utah and New Mexico. This is also corroborated by records I obtained and reviewed from Hashani.

36. On 2/27/2020, pursuant to the Administrative subpoena, Apple provided the following registration and subscriber information about the account: [badtrucking@icloud.com](mailto:badtrucking@icloud.com). The account was created on November 14, 2019 and is registered to Everett Miller of 176 Red Hill Road, Sunbright, Tennessee. The listed telephone for the account was 865-250-[REDACTED]. The

account was created using the IP address 17.110.67.415. There is also an iTunes account associated with the same registration. On 2/7/2020, the account accessed the iCloud photo library on three occasions. This was the most recent activity on the account.

#### **Forensic Analysis of Miller's iPhone**

37. On 4/28/2020 an FBI Digital Forensic Examiner conducted a query of three phones: the victim's Samsung and iPhone and Miller's iPhone.

38. On the Samsung cell phone belonging to the victim, there were two images located in the folder "DCIM/Camera" which contain relevant location data and whose metadata indicates they were taken with this device. These images are listed below:

- a. **20200102\_115000.jpg**: Metadata records this image was taken on 1/20/2020 at 11:50:00 AM local time at the location (35.030044, -106.954343). This image depicts a parking lot and building. According to Google Maps, these coordinates resolve to 6292 Interstate 40, Albuquerque, New Mexico.
- b. **20200102\_115006.jpg**: Metadata records this image was taken on 1/20/2020 at 11:50:06 AM local time at the location (35.030427, -106.952558). This image depicts a sign stating, "Route 66 Casino." According to Google Maps, these coordinates resolve to 6292 Interstate 40, Albuquerque, New Mexico.

39. The satellite view of the Google Maps website shows the Route 66 Casino Hotel in Albuquerque, New Mexico at or near both locations described in the metadata associated with the images described immediately above.

40. I also reviewed text messages on the victim's Samsung phone. On 1/2/2020 at 1:50 p.m., the victim texted [REDACTED] a photograph of the same casino noted above. The message above it said, "*I've also seen some huge casinos*".

41. In the two images listed above, the file naming convention, EXIF capture time, and file system modified time all match, and the EXIF camera makes and models are the same as the phone make and model (Samsung SM-J727V). This indicates these images were taken with this device.

42. Three other images were located in the folder "DCIM/Camera" which contain relevant location data. EXIF metadata indicates that all these photos were taken with an LG VS501 cell phone. The photos are listed below:

- c. **0701190854.jpg**: Metadata records this image was taken on 1/1/2019 at 8:54:33 AM local time at the location (39.053710, -94.476411). This image depicts a stadium and sign with the logo "KC". According to Google Maps, this location resolves to Interstate 70 in Kansas City, adjacent to the Kansas City Royals Baseball Stadium
- d. **0703191401.jpg**: Metadata records this image was taken on 1/3/2019 at 2:01:33 PM local time at the location (40.914273, -111.402810). This image depicts a body of water. According to Google Maps, this location resolves Interstate 80 in Coalville, Utah. Google Maps identifies the closest body of water as the Echo Reservoir.
- e. **0703191410.jpg**: Metadata records this image was taken 1/3/2019 at 2:10:19 PM local time at the location (40.913451, -111.402914). This image depicts a body of water. According to Google Maps, this location also resolves near Interstate 80 and Lincoln Highway in Coalville, Utah.

43. No relevant location data was located on the victim's Apple cell phone.

44. Based on my training and experience investigating crimes involving adults who have a sexual interest in children, I know that adults can manipulate a child victim through a process known as grooming. This includes manipulating victim's feelings by telling them they love them, trying to control with whom they talk and spend time, and make promises of gifts in order to keep their interest.

45. A review of the chats recovered from the victim's phone purchased by Miller shows evidence of grooming. For example, in the chat below, Miller wants the victim to tell him ■ also has a romantic interest in him. These chats occurred in January 2020. Miller is the gray colored chat. The victim's messages are denoted in blue.



4:46 PM



Ej >

Ok I need know honestly what  
me and u have

Are u wanting me

Yes

I have never love someone this  
much I love u

I know

I am so deeply in love with u  
and hope u are with me

Yeah

Ok u text me when can I love u  
and I am trying to give u a good  
life

I know you are I love you too

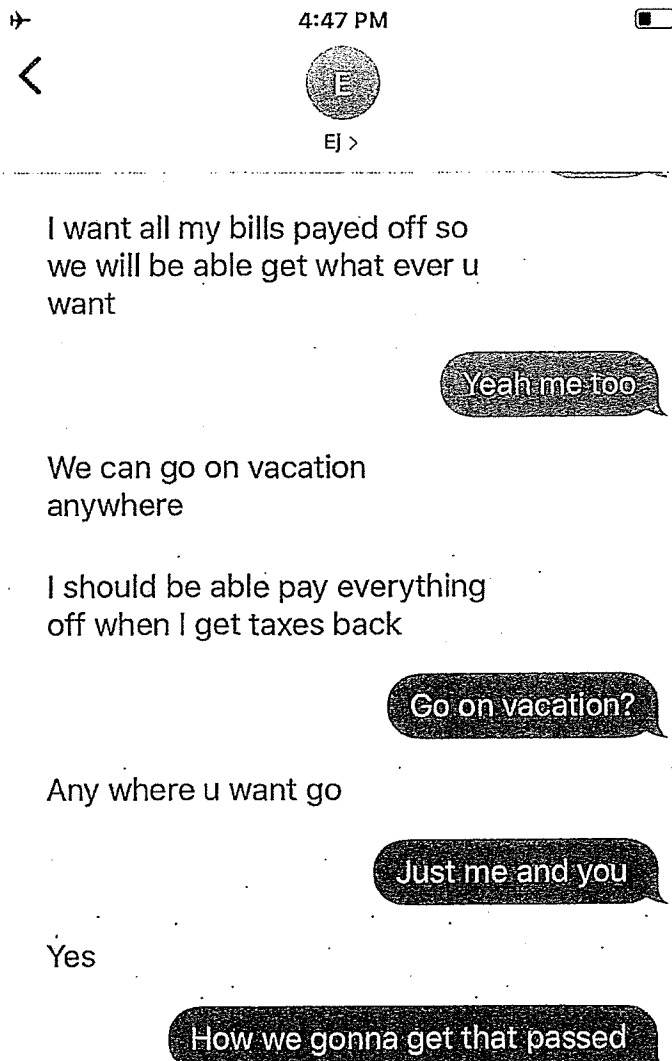
I will

Ok

Wed, Jan 15, 10:11 AM

I love u

46. Next, Miller made promises of gifts. In this chat, he offered to take the victim on an expensive trip after Miller received his tax refund, despite his anticipated objection by the victim's relatives. Miller also admitted he knew the victim was a minor by discussing how things will be better once [REDACTED] is an adult:



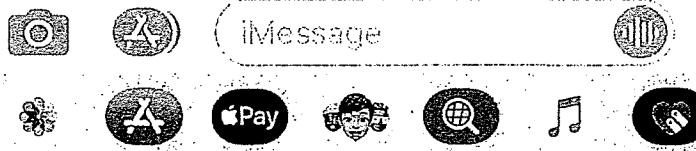
We will we say went salt lake  
Plus when u turn 18 go all time

Ok

That will work

Yes it will

Yeah



47. In several of the text exchanges between Miller and the victim, Miller professed his romantic love for the victim. The following is an excerpt from a text message exchange between Miller and the victim on January 16, 2020:



I want see u

I want to see you too

I have been lonely missing u  
today

Yeah just today?

No every minute of every day

That's sweet

I want u with me 24/7

U are what makes me happy

Yeah I know

I love u so much

I love you too

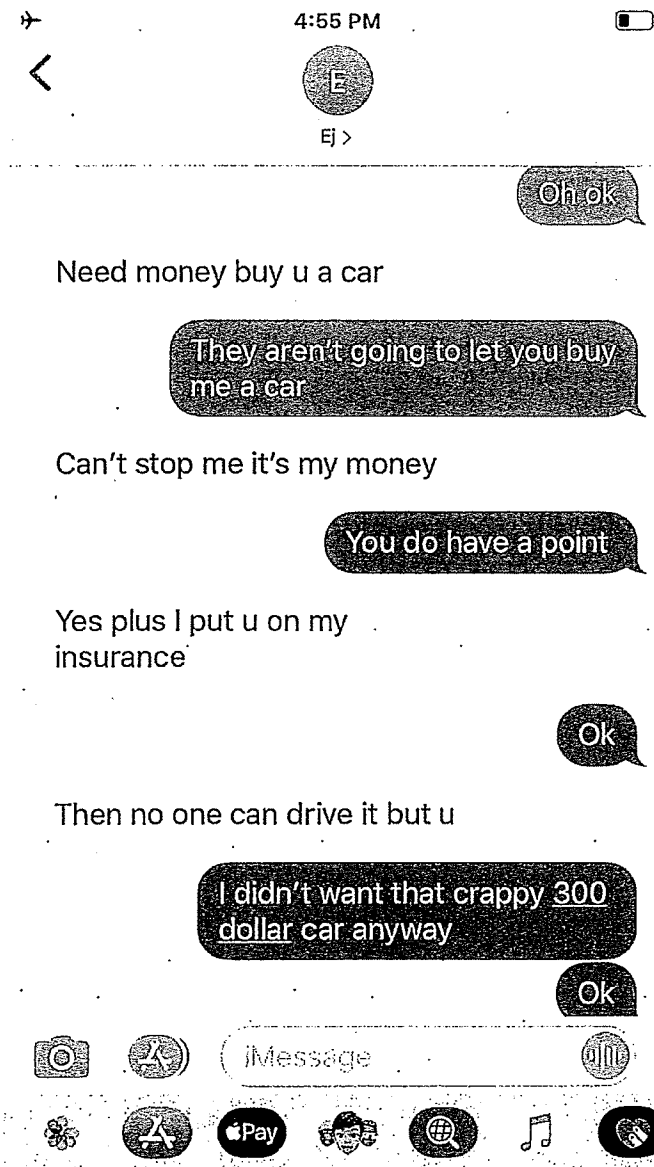
Every minute I think of u

I think of you too

I wish I was



48. Also, Miller continued grooming the victim by promising to purchase a nice car for the victim. The following is an excerpt from a text message exchange between Miller and the victim on January 22, 2020:





4:52 PM



Ej >

Ok baby night love with all my heart

Love you too

Til tomorrow n

Night



Wed, Jan 22, 7:49 AM

I miss u so much

I miss you too

I am trying make money

I know you are

That way get u a car

Yeah

I figured me and u can come up  
with enough we get u nice car

Text me when can love ❤️

Yeah i bet we could

I will love you too

That's what we will do

Ok

49. The following is an excerpt from a text message exchange between Miller and the victim on January 23, 2020:



4:54 PM



Ej >

Is that [REDACTED] leaving u alone

I want spend every minute with  
u

I will take care u forever if u  
want to be with me u will never  
want for anything I will make  
sure u are financially secure

All I ask be truthful and faithful  
and u will have everything

Thu, Jan 23, 11:27 AM

We haven't talked

Ok proud of u

U know I am deeply in love with  
u

I will to u are the most [REDACTED]  
[REDACTED] in world

No I'm not

Yes. u are and u are the  
smartest to

I am not smart

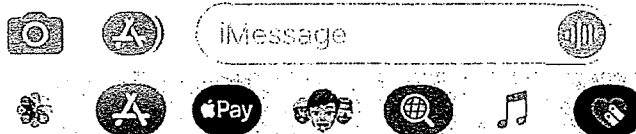
Yes u are

No I'm not

U smarter than me

No I'm not

I'm not smart enough to build  
stuff



Based upon my experience and training, Miller was exerting control over the victim by trying to prevent [REDACTED] from having a relationship with [REDACTED] and grooming [REDACTED] for sex by complimenting [REDACTED] on [REDACTED] and [REDACTED].

#### INFORMATION REGARDING APPLE ID AND iCloud<sup>1</sup>

<sup>1</sup> The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at <http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf>; "Create and start using an Apple ID,"

50. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

51. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications (“apps”). As described in further detail below, the services include email, instant messaging, and file storage:

f. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

g. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages (“iMessages”) containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

h. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

i. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and

---

available at <https://support.apple.com/en-us/HT203993>; “iCloud,” available at <http://www.apple.com/icloud/>; “What does iCloud back up?,” available at <https://support.apple.com/kb/PH12519>; “iOS Security,” available at [https://www.apple.com/business/docs/iOS\\_Security\\_Guide.pdf](https://www.apple.com/business/docs/iOS_Security_Guide.pdf), and “iCloud: How Can I Use iCloud?,” available at <https://support.apple.com/kb/PH26502>.

manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

- j. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.
- k. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.
- l. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.
- m. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.



52. Apple services are accessed through the use of an “Apple ID,” an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

53. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a “verification email” sent by Apple to that “primary” email address. Additional email addresses (“alternate,” “rescue,” and “notification” email addresses) can also be associated with an Apple ID by the user.

54. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including the user’s full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the “My Apple ID” and “iForgot” pages on Apple’s website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address (“IP address”) used to register and access the account, and other log files that reflect usage of the account.

55. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

56. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

57. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

58. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

59. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the offenses under investigation. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often

created and used in furtherance of criminal activity, including to communicate and facilitate the offenses under investigation.

60. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

61. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

62. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages,

Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crimes under investigation.

63. Given the facts articulated in this affidavit, it is reasonable to believe that information captured by Apple in its normal course of business, will confirm the travel of Miller and the victim, using Apple iPhones associated with the badtrucking@icloud.com account associated with both phones, thereby substantiating the victim's sexual assault disclosure. Through subpoena returns, Apple confirmed the iCloud account: badtrucking@icloud.com belongs to Everett Miller, for the dates pertinent to this investigation. It is reasonable to believe, based on photographs recovered through forensic examination at locations outside the State of Tennessee, observations of the iCloud account discovered in Apple iPhones utilized by both Miller and the victim, that records currently in the custody of Apple, will substantiate those facts. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the crimes under investigation including information that can be used to identify the account's user or users.

#### **INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED**

64. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

65. Based on the forgoing, I request that the Court issue the proposed search warrant.

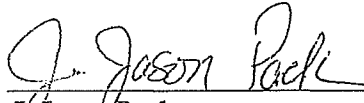
66. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

67. The government will execute this warrant by serving the warrant on Apple. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

REQUEST FOR SEALING

68. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,



J. Jason Pack  
Special Agent  
Federal Bureau of Investigation

Subscribed and sworn to before me on 5-15-2020, 2020



UNITED STATES MAGISTRATE JUDGE

**ATTACHMENT A**

**Property to Be Searched**

This warrant applies to information associated with badtrucking@icloud.com (the “account”) that is stored at premises owned, maintained, controlled, or operated by Apple, Inc., a company headquartered at Apple, Inc., 1 Infinite Loop, Cupertino, California 95014.

## ATTACHMENT B

### Particular Things to be Seized

#### I. Information to be disclosed by Apple

a. To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, Inc., (“Apple”) regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f), Apple is required to disclose the following information to the government, in unencrypted form whenever available, for the account described in Attachment A:

b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address), the date on which the account was created, the length of service, the IP address used to register the account, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers);

c. All records or other information regarding the devices associated with, or used in connection with, the account (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers (“UDID”), Advertising Identifiers (“IDFA”), Global Unique Identifiers (“GUID”), Media Access Control (“MAC”) addresses, Integrated Circuit Card ID numbers (“ICCID”), Electronic Serial Numbers (“ESN”), Mobile Electronic Identity Numbers (“MEIN”), Mobile Equipment Identifiers (“MEID”), Mobile Identification Numbers (“MIN”), Subscriber



Identity Modules (“SIM”), Mobile Subscriber Integrated Services Digital Network Numbers (“MSISDN”), International Mobile Subscriber Identities (“IMSI”), and International Mobile Station Equipment Identities (“IMEI”);

d. The contents of all emails associated with the account creation on 11/14/2019, through the most recent log-in on or about 2/7/2020, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails), the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

e. The contents of all instant messages associated with the account from 11/14/2019, through the most recent log-in on or about 2/7/2020, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages) sent to and from the account (including all draft and deleted messages), the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

f. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes), iCloud Tabs and bookmarks, and iCloud Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

g. All activity, connection, and transactional logs for the account (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

h. All records and information regarding locations where the account or devices associated with the account were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

i. All records pertaining to the types of service used;

j. All records pertaining to communications between Apple and any person regarding the account, including contacts with support services and records of actions taken; and

k. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

Apple is hereby ordered to disclose the above information to the government within fourteen days of issuance of this warrant.

## **II. Information to be seized by the government**

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of 18 U.S.C. § 2423(a) involving Everett Miller ("Miller") utilizing badtrucking@icloud.com, including, for each account or identifier listed on Attachment A, information pertaining to the following matters:

- a. Communications, including instant messages (including iMessages, SMS messages, and MMS messages) and voice mail messages between Miller and a minor victim utilizing telephone numbers 423-215-████ and 865-250-████;
  - b. Files exchanged between Miller and a minor victim, including voice recordings and digital image or movie files;
  - c. Evidence of preparatory steps taken in furtherance of the crime, including travel arrangements and route/stop research;
  - d. Evidence of Miller's interstate travel;
  - e. The identity of the person(s) who created or used the Apple ID, including records that help reveal the whereabouts of such person(s);
  - f. Evidence indicating how and when the account was accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crime under investigation and the activities of the account subscriber;
  - g. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information); and
  - h. Evidence indicating the subscriber's intent as it relates to the crimes under investigation;
- and

- i. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

**CERTIFICATE OF AUTHENTICITY OF DOMESTIC  
RECORDS PURSUANT TO FEDERAL RULES OF  
EVIDENCE 902(11) AND 902(13)**

I, \_\_\_\_\_, attest, under penalties of perjury by the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this certification is true and correct. I am employed by [PROVIDER], and my title is \_\_\_\_\_.

I am qualified to authenticate the records attached hereto because I am familiar with how the records were created, managed, stored, and retrieved. I state that the records attached hereto are true duplicates of the original records in the custody of [PROVIDER]. The attached records consist of \_\_\_\_\_ [GENERALLY DESCRIBE RECORDS (pages/CDs/megabytes)]. I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth by, or from information transmitted by, a person with knowledge of those matters, they were kept in the ordinary course of the regularly conducted business activity of [PROVIDER], and they were made by [PROVIDER] as a regular practice; and

b. such records were generated by [PROVIDER'S] electronic process or system that produces an accurate result, to wit:

1. the records were copied from electronic device(s), storage medium(s), or file(s) in the custody of [PROVIDER] in a manner to ensure that they are true duplicates of the original records; and

2. the process or system is regularly verified by [PROVIDER], and at all times pertinent to the records certified here the process and system functioned properly and normally.

I further state that this certification is intended to satisfy Rules 902(11) and 902(13) of the Federal Rules of Evidence.

---

Date

---

Signature